EXHIBIT 4

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS "THE CPS PREMISES" AND THE "DAVIDSON PREMISES" AT 1465 BROADWAY, HEWLITT, NEW YORK, AS DESCRIBED IN ATTACHMENT A

15 M 0688

SEALED AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

- X

STATE OF NEW YORK)
COUNTY OF KINGS :ss.:
EASTERN DISTRICT OF NEW YORK)

BRANDON W. McCAW, being duly sworn, deposes and says:

1. I am employed as a Special Agent with the United States Secret Service ("USSS") and I have been personally involved in the investigation of this matter. I am familiar with the facts and circumstances set forth below from my participation in the investigation of this case, from my personal knowledge, from my conversations with other law enforcement officers, and from my review of relevant documents. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they

are reported in substance and in part, except where otherwise indicated.

2. I have been a Special Agent with the Secret Service for more than one year. I have received training on electronic law and evidence, wire fraud, bank fraud, first-responder techniques in seizing computers and other electronic evidence, and on the uncovering and investigative uses of data. I have also been trained on debriefing of informants, search and arrest warrant operations, and witness interviewing.

3. This affidavit is respectfully submitted, pursuant to Federal Rule of Criminal Procedure 41, in support of an application for a warrant to search, as set forth in more detail below, the two premises (collectively, the "SUBJECT PREMISES") known and described as: (1) certain portions of the first floor and basement of 1465 Broadway, Hewlett, New York and closed cabinets and containers found inside (the "CPS PREMISES"); and (2) a one-room office of the firm of a certified public accountant, Michael Davidson, whose office is located within the CPS suite of offices (the "DAVIDSON PREMISES"). The CPS PREMISES are occupied by a credit card processing company that operates and has operated under the names Commerce Payment Systems, Commerce Payment Group, Merchant Commerce, Empire Payments, Evolution Bankcard, Optimal Bankcard and various other

names (collectively, "CPS"). The DAVIDSON PREMISES are the one-room office of accountant Davidson, who heads his own accounting business which handles much of CPS's accounting.

4. As set forth more fully below, there is probable cause to believe that MICHAEL MENDLOWITZ, a/k/a "Shmuel Mendlowitz," and other individuals working on behalf of CPS, (collectively referred to herein as the "TARGET SUBJECTS") have violated Title 18, United States Code, Sections 1343 and 1349 (the "TARGET OFFENSES"), among other statutes, by fraudulently overbilling CPS customers and collecting fraudulently inflated fees from CPS clients, through the use of the interstate wires.

Confidential Sources

5. This affidavit is based in part on my interviews of a cooperating witness ("CW-1") and a confidential source ("CS-1").

6. In an unrelated criminal case, CW-1 was charged in 2013 with violating federal criminal statutes that prohibit engaging in fraud. CW-1 has been cooperating with the Government in the instant investigation since approximately January 2015. CW-1 has pleaded guilty to various federal criminal charges, including participating in the TARGET OFFENSES at CPS, pursuant to a cooperation agreement with the Government, in the hopes of obtaining leniency at the time of sentencing.

CW-1 was employed at CPS from in or about April 2012 until in or about March 2015.

7. CS-1 was arrested on or about May 20, 2015 on a criminal complaint based on the criminal conspiracy and TARGET OFFENSES described herein. Since that date, CS-1 has been providing information to the Government in the instant investigation in the hopes of obtaining a cooperation agreement with the Government. CS-1 has been employed at CPS from in or about December 2010 up to and including the date of this affidavit.

8. CW-1 and CS-1 have provided detailed information about the fraudulent business practices, billing practices, sales practices, and customer agreements of CPS, as well as the role played in those fraudulent practices by the TARGET SUBJECTS. Information provided by CW-1 and CS-1 has been corroborated by, among other things, CPS agreements and bills, internal records, bank records, consensually recorded conversations, and information publicly available, including CPS's marketing materials and numerous customer complaints filed by merchant customers/victims of CPS with various government agencies and consumer complaint organizations.

THE SUBJECT PREMISES

9. The two SUBJECT PREMISES are inside a one-story, light grey building located at 1465 Broadway, Hewlett, New York ("the Building;" photographs of April 17, 2015 attached hereto as Attachment E). My fellow agents have viewed the building's exterior, which as recently as July 21, 2015, had three signs bearing the name "Commerce Payment Systems." One sign faces Broadway, while the other two face the reserved-for-tenants parking lot on the left side of the building. The Building has a single, main entrance, which is accessed through the parking lot on the left (northeast) side of the building. There is a secondary entrance on the front of the building, facing Broadway, which opens directly into the office of Michael Mendlowitz, the CEO of CPS. There is also another secondary entrance on the rear right-hand side of the Building. The Building contains several additional small businesses on the ground floor, including seven one-room businesses within the CPS suite.

10. As indicated in the ground-floor diagram attached hereto as Attachment D,[1] the CPS PREMISES include approximately five distinct areas within the Building: four on the ground

[1] I have prepared Attachment D, and the description in the following three paragraphs of the two SUBJECT PREMISES, upon information provided by CW-1 and CS-1.

floor (the main area, the computer/server room, the front cubicles, and the office of Michael Mendlowitz) as well as most of the basement of the building.

a. The main area. When entering the Building through the main door adjacent to the parking lot, the main area of the CPS PREMISES is straight ahead, mostly behind a reception area and wall. The main area fills a large essentially rectangular space, extending from the main entrance to the opposite wall, and from the right wall (adjacent to Broadway) to the left wall at the rear of the Building.

b. The computer/server room. Along the left-hand (southeast) wall of the main area of the CPS PREMISES is a short hall going to the left. Off that hall, on the right-hand side, is the computer/server room. On the left-hand side of that hall is a set of stairs that leads down to the basement.

c. The basement. A portion of the CPS PREMISES is in the basement of the Building. After one descends the stairs mentioned in the preceding paragraph, one encounters a file storage room on the immediate left, with an adjacent storage area. The next two rooms contain CPS's customer

service and shipping departments, each of which also has an adjacent storage area.

d. The front cubicles. Back on the ground floor, if one turns left upon entering the main door of the building from the parking lot, the front cubicles are on the left. Several yards beyond that are three computers and cubicles belonging to employees engaged in the "boarding" process, by which customer profiles are created and loaded with customer-specific information, including fee information.

e. The office of Michael Mendlowitz. Along the right-hand, northwest wall of the main area, adjacent to Broadway, is the office of Michael Mendlowitz. It is approximately the fifth room along that wall, after two one-room offices of other businesses, a CPS conference room, and one more one-room office of another business.

11. As further indicated in the ground-floor diagram attached hereto as Attachment D, the DAVIDSON PREMISES consist of the one room office of accountant Michael Davidson, which is within the CPS suite of offices. According to CS-1, the DAVIDSON PREMISES are immediately to the right after one enters the CPS PREMISES via the main door of the building from the parking lot. According to CW-1 and CS-1, Davidson is not

employed by CPS, but he is the accountant primarily responsible for handling many of CPS's accounting matters.

12. In addition to the two SUBJECT PREMISES, the ground floor of the Building contains approximately six small one-room business offices leased by other small businesses, which are shaded in gray on Attachment D. These are not within the ambit of this application. One of these small offices is on the immediate right as one enters the building through the main entrance from the parking lot. Three more — as described in paragraph 8(e), above — are along the right-hand, northwest wall of the building, facing Broadway (as is a CPS conference room, which is the third room). The other two one-room businesses leased by outside entities are toward the left as one enters the building through the main entrance, adjacent to the front cubicles described above.

PROBABLE CAUSE

CPS and its Affiliates

13. In the course of this investigation, I have reviewed various records, including public records, complaints filed by merchant customers/victims of CPS with various government agencies and consumer complaint organizations; bank records, customer bills from CPS, and customer agreements of CPS. From these records and from my interviews of CW-1 and CS-1, I have

learned that since at least in or about 2010, up to and including the date of this Affidavit, CPS, using various names, has operated out of the CPS PREMISES. During this time, CPS has operated as a credit card servicing company, servicing credit cards, debit cards and bank cards (referred to herein collectively as "cards") for its customers, who are merchants that accept such cards from the purchasing public. As a card service company, CPS has acted as an intermediary between the merchants and various banks and providers of cards, performing such functions as gathering information about merchants and their sales, handling the consolidation of revenue from commercial transactions, reconciling accounts, and taking out fees.

14. CPS performs some of these functions together with EVO Merchant Services, LLC, a company that holds a substantial stake in CPS and which is also affiliated with EVO Payment Systems (collectively referred to herein as "EVO"). For example, the agreements with CPS customers are presented to customers by CPS sales personnel as agreements with CPS, and prominently feature the name and logo of Commerce Payment Group. The substantive fine print of those agreements, however, refers to EVO. Bank records likewise reflect that much of the revenue from CPS customers flows to a bank account in the name of EVO, and many

of CPS's bills and payroll expenses are paid out of that EVO account.

Key Individuals and Entities

15. I have interviewed CW-1 and CS-1 about the role played at CPS by TARGET SUBJECT Michael Mendlowitz, a/k/a "Shmuel Mendlowitz," and others, as well as by the accountant Michael Davidson. From at least 2012 up to and including the date of this Affidavit, Michael Mendlowitz has functioned as the CEO and principal of CPS, purportedly holding a minority ownership share in CPS. Mendlowitz plays a central role in developing and implementing CPS's customer service, customer retention, sales, and billing practices, as well as overseeing staff, particularly staff involved with CPS's sales, customer service, customer retention, and billing practices.

16. From in or about at least 2012 until in or about at least March 2015, most of CPS's accounting has been handled by Michael Davidson, an accountant who operates his own firm in the DAVIDSON PREMISES, which is within the CPS suite of offices. Among other things, Davidson has handled CPS's accounting matters and payroll, as well as aspects of the financial relationship between CPS and EVO. Employees of CPS have often been directed to speak to or contact Davidson regarding CPS accounting issues. In addition, Davidson has regularly met with

Michael Mendlowitz and communicated with representatives of EVO, about CPS accounting issues. The bank records of CPS and EVO reveal that the financial affairs of CPS and EVO are closely intertwined. For example, most of the fees paid by victim customers of CPS go first through the bank accounts of EVO, before being transferred to the bank accounts of CPS. Accordingly, there is probable cause to believe that the DAVIDSON PREMISES contains financial records of CPS that will reflect financial transactions, debits and credits between EVO and CPS; supporting documentation for such transaction, debits and credits; commissions (or "residual payments") from EVO to CPS and to other recipients of proceeds of the TARGET OFFENSES; and the location of proceeds of the TARGET OFFENSES.

Previously Issued Search Warrant

17. This is the second application in this investigation for a search warrant for the CPS PREMISES and the DAVIDSON PREMISES. The first application was granted on May 13, 2015 by Hon. James Orenstein, United States Magistrate Judge, who issued a search warrant to be executed on or before May 27, 2015. However, subsequent developments in the investigation caused the Government to reconsider the timing of the search and to conclude that the investigation would be better served by delaying the search. Among other things, shortly after that

search warrant was issued, on May 19-20, 2015, the Government arrested and met with CS-1, who began engaging in proactive efforts at cooperation with the Government.

The Scheme to Defraud

18. Publicly available records, along with detailed information provided by CW-1 and CS-1, reveal that CPS actively markets its business through the internet, flyers, and telephone calls. CW-1 and CS-1 report that initial marketing calls are often made by third-party contractor companies, who in turn refer calls from prospective customers to CPS's sales force. CPS's sales force is instructed by CPS management on how to approach potential customers, using daily practice sessions and pre-written scripts, which I have reviewed, that contain specific false representations about how the customer will be billed. In addition, according to CW-1, when potential customers contact CPS, sales personnel are instructed to work directly with them in filling out their applications/agreements, walking them quickly through the documents, while making false representations to them about how they will be billed.

19. In the course of its business, the TARGET SUBJECTS, together with others known and unknown, have caused CPS and its employees to use a variety of fraudulent means to charge customers improper fees, typically totaling approximately two or

three times the charges represented by CPS during the sales process and as set out in the customers' agreements. These mechanisms have been described to me by CW-1 and CS-1, and corroborated by my review of customer bills and agreements. In addition, CW-1 and CS-1 discussed them in detail during the consensually recorded conversation of January 28, 2015, at which time CS-1 was still participating in the SUBJECT OFFENSES. Such improper fees have been imposed through a number of different fraudulent mechanisms, including:

a. over-billing customers by charging overall commission fees at percentage rates that are higher than the commission percentage rates set forth in CPS's marketing materials, CPS's representations to customers, and in the customers' agreement with CPS and EVO;

b. over-billing customers for a number of commissions when only one commission may properly be charged under the terms of a customer's agreement and according to the representations that CPS sales staff make to customers during the sales process, while also adding unjustified surcharges to such fees;

c. billing customers multiple times for "transaction fees" on a single commercial transaction, so that the CPS customer pays as many as five different

transaction fees for a single commercial purchase, when such fee can properly be charged only once under the terms of the customer's agreement and according to CPS's marketing materials and sales representations;

d. billing a customer for a "Payment Card Industry" (PCI) compliance fee, purportedly for protective and insurance services, which services CPS had not in fact procured for the customer;

e. billing a customer for "dues and assessments" on all sales, when in fact such fees were properly charged on only a limited number of sales;

f. billing a customer for various other surcharges, including on transactions where there was no basis for such surcharges and when customers were explicitly told that they would not be charged such fees;

g. continuing to charge customers for unwarranted fees even after a customer repeatedly instructed CPS to terminate the customer's relationship with CPS; and

h. failing to pay customer full refunds, even when the customer demonstrated that it was entitled to such refund.

20. In addition, the TARGET SUBJECTS, together with others known and unknown, have taken a variety of steps to conceal

CPS's overbilling from CPS's customers. These means of concealment have been described to me by CW-1 and CS-1, and corroborated by my review of customer bills and agreements, customer complaints, and publicly available marketing materials. In addition, CW-1 and CS-1 discussed them in detail during the recorded conversation of January 28, 2015. These steps have included:

a. mislabeling various charges in a bill, such as labeling purely internal fees as "Visa Assessments" or "MasterCard Assessments," or greatly overstating the size of fees imposed by third-party card providers;

b. intentionally concealing the cumulative effect of the various fraudulent fees by causing them to appear in different parts of a victim/customer's bill, with some of the fees withheld from initial payments while others appear in various other parts of the same bill; and

c. hiding transaction fees and access fees within other larger fees, which were in turn misleadingly labelled, and without any distinction made between fees charged by percentage and flat monetary fees, nor between percentage figures and dollar amounts; and

d. limiting customer access to their own bills - without notice to the customers - by failing to send bills

out to customers unless the expressly request them, and failing to make bills available to customer's online unless the customer expressly asked for such access, without telling customers that access to their bills will be so limited and without notifying customers that the fees will be withdrawn directly from their bank accounts without a bill being sent.

21. In the course of this scheme, the TARGET SUBJECTS, together with others known and unknown, have taken steps to insure that the marketing claims made to prospective customers in general solicitation materials and in scripted one-on-one sales conversations are materially false and misleading. These fraudulent marketing practices have been described to me by CW-1, and corroborated by my review of customer complaints, CPS marketing materials, written scripts for CPS sales personnel, and CPS bills and agreements. This fraudulent conduct includes:

a. providing CPS's sales personnel with prepared written scripts and explicit instructions, which I have reviewed, telling potential customers that there are no fees beyond the basic percentage and 10-cent transaction charge, and that all fees were fixed for the life of the relationship, when in fact -- as revealed in customer bills and recorded admissions -- CPS charged a variety of additional usage fees, multiples of

fees, fees at much higher rates, and inactivity fees, often to customers to whom these fees did not properly apply;

b. providing CPS's sales personnel with written scripts, bonus incentives, and daily coaching sessions, instructing them on high-pressure sales techniques that are intended to limit the opportunity for the prospective customer to scrutinize or confirm CPS's representations before signing its application/agreement;

c. using false names when identifying themselves to customers;

d. instructing CPS's sales personnel on the use of a website-based "cost comparison calculator," and on how to use those website demonstration screens to show a customer what their prospective bills are purportedly projected to be, when in fact the numbers and fees in that calculator were dramatically lower than the actual bills later sent to customers;

e. distributing written and internet marketing materials, which I have reviewed, stating: "No hidden fees - Ever!" with an accompanying schedule of a few simple low fees that are well below the fees that CPR actually charges;

f. providing letters to new customers stating: "Important Note: Each and every rate that is agreed on this

application will be set in for the lifetime of the account, regardless of the fact that there is no long term agreement."

g. distributing written and internet marketing materials stating: "Your Statements Are Clear and Simple. We promise that you will be able to read your statement and understand every line of it."

h. distributing written and internet marketing materials stating: "You'll never have to worry about hidden fees, escalating rates or any set up costs - because there aren't any!" with an accompanying fraudulently incomplete schedule of a few simple low fees.

22. From at least in or about 2012 until in or about January 2015 -- as detailed by CS-1 and CW-1 and corroborated by bank records, complaint files and customer agreements -- the TARGET SUBJECTS, together with others known and unknown, operated the on-line application process for prospective CPS customers in a manner that insured that applicant customers saw only a two-page agreement. This process has been described to me by CW-1 and CS-1, and corroborated by my review of customer complaints and accompanying documentation.

a. When customers later complained that their agreements had been breached, CPS sometimes claimed that its customer agreements contained an additional three pages of

"terms and conditions" that allowed for unilateral rate increases. Significantly, these undisclosed terms and conditions purportedly reserved to CPS various rights that were in direct contradiction of oral and written representations that CPS made to customers and prospective customers. For example, the terms and conditions, a version of which I have reviewed, provided that (i) any prior representations to the customer were superseded; (ii) fees could be added or increased despite explicit prior promises by CPS representatives that fees could not be increased.

b. As CW-1 and CS-1 have explained, the TARGET SUBJECTS insured that CPS did not disclose, make available, or show these "terms and conditions" to customers or prospective customers, providing instead a two-page email attachment and link that omitted those pages. This is corroborated by my inspection of complaint files submitted by defrauded CPS customers to the New York State Attorney General's Office, which reveals that each of the six complaints that contain a customer agreement shows that the customer was provided only a two-page agreement, without the additional pages containing the supposed "terms and conditions."

23. From in or about at least 2010 until in or about at least July 2015, CPS periodically used different company names to conduct its business. In addition to "Commerce Payment Systems" and "Commerce Payment Group," these names included "Merchant Commerce," "Empire Payments," "Evolution Bankcard," and "Optimal Bankcard." Web pages and marketing materials for each of these entities can be found on the internet, generally with web pages similar to that of Commerce Payment Systems. CW-1 and CS-1 have explained that these additional company names and identities were created by the TARGET SUBJECTS, together with others known and unknown, in order to counter the negative business effect that Commerce Payment Systems suffered – and in turn that Evolution Bankcard and the other companies eventually suffered –from an increasingly negative reputations on the internet, caused by a large number of on-line consumer complaints, as well as low evaluation ratings on various websites, and poor customer ratings.

24. From in or about at least 2012 until in or about at least March 2015, the TARGET SUBJECTS, together with others known and unknown, took various steps to conceal the relationship between these various CPS-affiliated companies, as CW-1 has explained and as is evident on their respective websites and marketing materials. So, for example, when these

new company names and identities were created and implemented, CPS operated multiple telephone lines at the same office, with the same employees identifying their corporate affiliations differently, depending on what telephone number the prospective customer had called or what internet advertisement had generated the referral. In addition, CPS personnel took care to create different email addresses for its employees, depending on which company they were purporting to represent, and to ship out its card processing equipment using differently labelled boxes and different delivery labels, in order to conceal the relationship between Commerce Payment and the other CPS-affiliated companies. And although each of the new companies operated out of the CPS PREMISES in Hewlett, New York, CPS personnel created the new websites to list different telephone numbers and different addresses, such as the address of EVO, or no address at all.

Over-billing of Individual Victim/Customers

Victim-1

25. Based upon my review of the CPS agreement entered into with one merchant customer ("Victim-1") in or about July 2014, and the bill charged to that customer in or about December 2014, I have learned the following:

a. In total, Victim-1's December 2014 bill reflects charges of $838.03 -- obscured by the way the charges are set

out differently in different parts of the bill -- which greatly exceed the contracted amount as provided in Victim-1's agreement with CPS. This overbilling was achieved through a variety of fraudulent mechanisms. For example:

b. Victim-1's agreement provides that Victim-1 will be charged a base percentage rate of 1.33% on credit card transactions or 0.23% on debit card transactions. But in fact Victim-1's bill reflects that Victim-1 was billed a base rate of 1.39% on all transactions, whether credit or debit. Moreover, Victim-1 was then then additionally charged a "network access" or "integrity fee" of 1.33%. So all together, Victim-1 was billed a base percentage rate of 2.72% on all transactions, whether credit or debit.

c. Victim-1's agreement provides that Victim-1 will be charged a flat transaction fee of 6 cents per transaction. But in fact Victim-1's bill reflects that Victim-1 was billed three separate transaction fees, respectively for 10, 15, and 10 cents - totaling 35 cents. These three fees on each transaction were labelled in three different ways.

d. Victim-1's agreement provides that Victim-1 will be charged 1.95 cents per transaction as a "Visa [or MasterCard or Discover] Authorization/Settlement Network

Access/Usage Fee." But in fact Victim-1's bill reflects that Victim-1 was charged two such fees, and that each fee was for 19.5 cents, totaling 39 cents rather than the 1.95 cents. Thus, Victim-1 was billed twenty times the amount of the access fee per transaction provided for in its agreement.

e. Victim-1's agreement provides that Victim-1 can be charged a "surcharge" of 2.75% plus 10 cents on certain "non-qualified" transactions charged on certain types of cards. But in fact Victim-1's bill reflects that Victim-1 was charged a surcharge of 2.95% plus 10 cents on every transaction, regardless of whether or not the transaction was a non-qualified transaction.

Victim-2

26. Based upon my review of the agreement entered into with another merchant customer ("Victim-2") in or about November 2012, and the bill charged to that customer in or about November 2014, I have learned the following:

a. In total, Victim-2's November 2014 bill reflects charges of $558.72 -- obscured by the way the charges are set out differently in different parts of the bill -- which greatly exceed the contracted amount as provided in Victim-2's agreement with CPS. This overbilling was achieved through a variety of fraudulent mechanisms. For example:

b. Victim-2's agreement provides that Victim-2 will be charged a base percentage rate of 1.40% on credit card transactions or 0.35% on debit card transactions. But in fact Victim-2's bill reflects that Victim-2 was billed a base rate of 1.59% on all transactions (whether credit or debit). Moreover, Victim-2 was then additionally charged a "network access fee" of 1.59%. So all together, Victim-2 was billed a base percentage rate of 3.18% on all transactions, whether credit or debit.

c. Victim-2's agreement provides that Victim-2 can be charged "dues and assessments" at a rate of up to .095%. But in fact Victim-2's bill reflects that Victim-2 was billed assessments of .95%, or ten times the rate provided in Victim-2's agreement.

d. Victim-2's agreement provides that Victim-2 will be charged a flat transaction fee of 10 cents per transaction. But in fact Victim-2's bill reflects that Victim-2 was billed three separate transaction fees, each for 20 cents, totaling 60 cents. These three fees on each transaction were labelled in three different ways, with one of them merged with a percentage fee that obscured the second charge.

e. Victim-2's agreement provides that Victim-2 will be charged 1.95 cents per transaction as a "Visa [or MasterCard or Discover] Authorization/Settlement Network Access/Usage Fee." But in fact Victim-2's bill reflects that Victim-2 was billed two such fees, and that each fee was for 19.5 cents, totaling 39 cents rather than the 1.95 cents. Thus, Victim-2 was billed twenty times the amount of the access fee provided for in its agreement.

f. Victim-2's agreement provides that Victim-2 can be charged a "surcharge" of 1.92% plus 10 cents on certain "non-qualified" transactions charged on certain types of cards. But in fact Victim-2's bill reflects that Victim-2 was billed a surcharge of 2.95% plus 10 cents on every transaction, regardless of whether or not the transaction was a non-qualified transaction.

g. Although Victim-2's agreement does not provide for any "reporting fee," Victim-2 was billed $99.00 for such a fee. When customers call to inquire about such a fee, according to CS-1, they are told that it is the charge for generating an IRS 1099 form, although no such fee is provided for in the customer agreement.

Victim-3

27. Based upon my review of the agreement entered into with another merchant customer ("Victim-3") in approximately January 2013, and the bill charged to that customer in approximately December 2014, I have learned the following:

a. In total, Victim-3's December 2014 bill reflects charges of $1,253.47 -- obscured by the way the charges are set out differently in different parts of the bill -- which greatly exceed the contracted amount as provided in Victim-3's agreement with CPS. This overbilling was achieved through a variety of fraudulent mechanisms. For example:

b. Victim-3's agreement provides that Victim-3 will be charged a base percentage rate of 0.25% above an "interchange rate" set by card providers such as Visa and MasterCard. But in fact Victim-3's bill reflects that Victim-3 was billed this base rate of .25% above the interchange rate, then additionally charged a "Visa [or MasterCard] network access fee" of 0.95%. So all together, Victim-3 was billed a base percentage rate of 1.20% above the interchange rate, rather than the .25% provided in its agreement.

c. Victim-3's agreement provides that Victim-3 can be charged "dues and assessments" at a rate of up to .095%. But in fact Victim-3's bill reflects that Victim-3 was billed

assessments of .95%, or ten times the rate provided in Victim-3's agreement.

d. Victim-3's agreement provides that Victim-3 will be charged a flat transaction fee of 10 cents per transaction. But in fact Victim-3's bill reflects that Victim-3 was billed three separate transaction fees, each for 20 cents, totaling 60 cents. These three fees on each transaction were labelled in three different ways, with one of them merged with a percentage fee that obscured the second charge.

e. Victim-3's agreement with CPS provides that Victim-3 will be charged 2 cents per transaction as a "Visa [or MasterCard or Discover] Authorization/Settlement Network Access/Usage Fee." But in fact Victim-3's bill reflects that Victim-3 was billed two such fees, and that each fee was for 19.5 cents, totaling 39 cents. Thus, Victim-3 was billed 19.5 times the amount of the access fee provided for in its agreement.

f. Victim-3's agreement with CPS provides that Victim-3 can be charged a "surcharge" plus 10 cents on certain "mid-qualified" or "non-qualified" transactions charged on certain types of cards. But in fact Victim-3's

bill reflects that Victim-3 was billed this surcharge plus 10 cents on every transaction, regardless of whether or not the transaction was mid-qualified or non-qualified.

g. Victim-3 was billed $39.95 for an "inactivity fee" - purportedly applicable where the customer does less than $35 worth of card business in a given month, despite submitting card charges totaling more than $25,000 that month and despite being billed by CPS more than $1,200 in that month.

Interstate Wires in Furtherance of the Fraud Scheme

28. Based on my review of customer complaints, customer files and bank records, as well as my interviews of CW-1 and CS-1, I have learned that -- since at least in or about 2010 through in or about July 2015 -- CPS has had customers throughout the United States, and that CPS personnel have carried out the business of CPS through the extensive use of interstate wire communications. As a general practice, CPS first contacts potential customers through interstate telephone calls and internet marketing, as detailed above. When potential customers express interest during the telephone call, CPS personnel work with them via a website, where the CPS sales representative and the potential customer jointly fill out on-line customer application forms. Following such interstate

telephone calls, CPS personnel typically email prospective customers a completed version of their customer application. Customer files indicate that, during the initial application process, CPS personnel had interstate telephone conversations and interstate wire communications with the following victims:

a. On or about July 31, 2014, CPS sales personnel in New York had telephone and internet communication with a representative of Victim-1 in Utah.

b. On or about November 30, 2012, CPS sales personnel in New York had telephone and internet communication with a representative of Victim-2 in Missouri.

c. On or about January 2, 2013, CPS sales personnel in New York had telephone and internet communication with a representative of Victim-3 in North Dakota.

29. I have learned through my review of bank records, including records of accounts maintained by CPS and EVO in New York, New York, that CPS's banking is carried out through extensive use of interstate wires. Typically CPS obtains its fees by causing customer funds to be wired directly from customer bank accounts throughout the United States to bank accounts of EVO in New York, New York. There, the funds are

used, among other things, to pay CPS bills and operating expenses. For example:

a. On or about December 2, 2014, $303.48 was transferred by wire from the bank account of Victim-2 in Missouri to a bank account in New York, New York, for the benefit of CPS.

b. On or about August 4, 2014, $54.78 was wired from a bank account of a merchant customer ("Victim-4") in Oklahoma to a bank account in New York, New York, for the benefit of CPS.

c. On or about September 3, 2014, $278.18 was wired from a bank account of Victim-4 in Oklahoma to a bank account in New York, New York, for the benefit of CPS.

d. On or about July 2, 2013, $118.95 was wired from a bank account of a merchant customer ("Victim-5") in New Hampshire to a bank account in New York, New York, for the benefit of CPS.

e. On or about July 16, 2014, $180,418.92 was transferred by wire from a bank account of EVO in New York, New York to an account at a bank in Connecticut, to pay payroll to CPS's employees.

Recorded Conversation

30. I and my fellow agents have listened to six consensual recordings, recorded between January 28 and May 29, 2015. The January 28 conversation consists largely of CS-1 (who was then still participating in the subject offenses) explaining to CW-1 (who was in the process of assuming new job responsibilities) how some of CPS's fraudulent overbilling practices are carried out, both to improperly overbill customers and to keep customers from discovering that they are being overbilled. CS-1 also explained - in both the January 28, 2015 and February 11, 2015 conversations - that TARGET SUBJECT Michael Mendlowitz knew and approved of the mechanisms used for fraudulent overcharges.

31. In the recorded conversation of January 28, 2015, CS-1 stated that:

a. CS-1 and other CPS personnel took steps - contrary to the representations made to customers and reflected in the customers' agreements - to insure that CPS billed all customers the highest commission rate of 2.95% on all transactions, even though only 40% to 45% of those transactions were "non-qualified" transactions subject to that highest rate. CS-1 stated: "It could be the cleanest card in the world, and we'll still charge 2.95% (Laughs). Thanks to me bro, I've been making Michael [Mendlowitz] a lot of money because of that."

b. CS-1 insures that CPS's bills are intentionally structured so that the customer gets billed for as many as five different "transaction fees" on a single transaction. The co-conspirators carry out this overcharging on approximately 900,000 transactions per month, resulting in hundreds of thousands of dollars of illicit profits.

c. CS-1 and one or more of his co-conspirators insure that CPS fraudulently charges customers a "membership fee," often mislabeled as a "maintenance fee," which the customers do not understand they are being charged;

d. In total, the cumulative fees and commissions that CPS bills to customers typically add up to between 7% and 10% of customers' own sales - far in excess of the rates provided in their agreements with CPS;

e. "If we don't f**k them, somebody else is going to f**k them. Might as well let us f**k them. . . . Other companies are going to slam them some way somehow. Not as aggressive as we are, though."

f. "We try to confuse the merchant as much as we can, obviously. (Laughs). We charge 1 10-cent transaction fee on a daily basis with the qualifying rate. That's one. We charge a 10-cent transaction fee on the dues and assessments. That's two. We charge a transaction fee on

the surcharge. That's three. We charge a regular transaction fee. That's four. We charge a network access transaction fee. Again. That's five. So really the merchant's paying 50 cents per transaction.

CW-1: "Wow, instead of the 10 cents they think?"

CS-1: Yeah. We got away with it, to be honest. So, do the math, Bro. Michael [Mendlowitz] does like 900,000 transactions [per month], times 50 cents. That's transaction fees only."

* * *

CW-1: "So, what's a membership fee?"

CS-1: "It's just BS. We tell the merchants it's like a maintenance fee. Or we call it a licensing fee from issuing banks which will enable the credit card processing. They fall for that sh*t."

Electronically Stored Information:
Means of Communication, Document Preparation, and Filing

32. In the course of my this investigation, I have learned the following from my interviews of CW-1 and CS-1 and an internet service provider, as well as from my review of various records, including public records, complaints filed by merchant customers/victims of CPS with various government agencies and consumer complaint organizations, customer bills from CPS, and

customer agreements of CPS. Much of the business of CPS is conducted through electronic means, and much of the evidence of this business conduct resides in electronic media. For example, CPS employees accept initial customer applications (which become customer agreements) through web-based software, links and email attachments, which the customers sign electronically. Copies of those agreements are stored electronically, and also are transmitted to other locations, including EVO. Similarly, most customers' billing statements are prepared and stored electronically. Some small portion of the customer billing statements is also sent out by mail. Other correspondence and file notes pertaining to particular customer files are stored on one or more computer servers at the CPS PREMISES.

33. In addition, I have learned from CS-1 and CW-1 that CPS and its employees make extensive use of desk-top computers, portable personal computers, personal digital assistants, smart telephones, e-mails and mobile telephone texts to carry out their operations and to further the fraud. TARGET SUBJECT Michael Mendlowitz uses e-mails to communicate company practices, as do other CPS supervisors, and use e-mail, mobile telephone texts, electronic document sharing, and other electronic media to communicate with each other. Similarly, most of the written correspondence within CPS and between CPS

and its customers, accountant Michael Davidson, banks and other service providers is sent via-email, and other communication being prepared on CPS computers. TARGET SUBJECT Michael Mendlowitz, as well as his co-conspirators and other CPS employees, store documents on their computers, portable personal computers, and smart telephones.

34. I have learned from CS-1 that, until in or about 2013, CPS also maintained a printed customer file for each customer. These paper files have since been stored in the basement storage areas of the CPS PREMISES.

35. As to telephone conversations, I have learned from CS-1 and CW-1 that it is the practice of CPS to record both internal and external telephone conversations, and to store those recordings electronically on one or more computer servers in the computer server room. In addition, TARGET SUBJECT Michael Mendlowitz uses a separate phone system, available to only a handful of CPS employees.

36. From my review of bank records and conversations with banking representatives, I have also learned that the business, financial, and banking affairs of CPS are closely intertwined with those of EVO. For example:

a. most of the fees collected are initially transferred by wire to accounts of EVO in New York, New York and elsewhere;

b. many of CPS's daily operating expenses are paid directly out of a bank account that is funded almost entirely by daily transfers of money from a bank account of EVO;

c. some of CPS's expenses - such as bi-weekly employee payroll - are paid directly out of a bank account in the name of EVO;

d. in a bank account in the name of Commerce Payment Group at a bank in New York, New York, most of the authorized signatories on the account - in addition to Michael Mendlowitz - are officers and executives of EVO; and

e. in bank records and other official documents, CPS frequently uses EVO's corporate address (515 Broadhollow Road, Melville, NY 11747) as CPS's own, rather than CPS's true address at 1485 Broadway, Hewlitt, New York.

37. Based on my training and experience, I also know that individuals who engage in complex corporate wire fraud commonly use computers to communicate on line with, *inter alia*, co-conspirators, service providers, banks, victims and potential victims; to access websites used for illegal activity; keep track of contact information of co-conspirators, service

providers, banks, victims and potential victims; to keep a record of illegal transactions or criminal proceeds for future reference; to store data for future exploitation; and for other purposes. As a result, they often store data on their computers related to their illegal activity, which can include email correspondence; customer files; lists of customers and potential customers; logs of online "chats" with co-conspirators and customers; contact information of co-conspirators, service providers, banks, victims and potential victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions or the disposition of criminal proceeds.

38. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

Items Likely to Be Found at the SUBJECT PREMISES

39. In light of the foregoing, there is probable cause to believe that the two SUBJECT PREMISES and each computer or other storage medium therein contain electronically stored and documentary evidence, fruits, instrumentalities and proceeds of a fraudulent credit card processing operation, including, but not limited to:

a. business and financial reports and records, bank and credit card records, customer contracts and applications, customer bills, customer billing profiles, sales and debt-collection records, employee records and

files, spreadsheets, ledgers, call logs, call lists, service and other contracts, recorded telephone calls, creditor and debtor records, internal and external correspondence and communications, mail, and payment records, among other documents, stored media and records.

b. checks, customer contracts and agreements, customer bills, copies of canceled checks, cash, money orders, records of credit card payments, mail, mail envelopes, correspondence, communications, faxes, emails, phone records (including digital and/or VOIP records), receipts, invoices, general journals, ledgers, financial reports, spreadsheets, memoranda, and notes.

c. Bank account and transaction documents, including account opening documents, ATM and/or debit cards, bank statements, and bank deposit and withdrawal slips;

d. Customer and/or debtor lists, customer and/or debtor files, lists of names, addresses, social security numbers, contact information, bank account numbers, credit card numbers and other personal identifying information, records of communications with customers and/or debtors;

e. Company policies, manuals, instructions, and/or scripts;

f. Licenses and/or registrations;

g. Documents, records and policies regarding employee compensation, such as bonuses and/or commissions;

h. Payroll records, employee names, personnel files;

i. Documents or records bearing the names "Commerce Payment Systems," "Commerce Payment Group," "Merchant Commerce," "Empire Payments," "Evolution Bankcard," "Optimal Bankcard," "EVO Merchant Services," "EVO Payments International," "Michael Mendlowitz," or similar names;

j. Records relating to and communications regarding lenders, creditors and/or other sources of information regarding debtors or debts to be collected; and

k. Computer(s), computer hardware, software, related documentation, and passwords.

Procedures for Searching Electronically Stored Information ("ESI")

A. Execution of Warrant for ESI

40. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take

considerable time and resources for forensic personnel to detect and resolve.

B. The Davidson Office

41. As discussed herein, the accounting office of Michael Davidson (the "Davidson Office") is within the CPS suite of offices and is part of the SUBJECT PREMISES. Davidson serves as an accountant for CPS. In contrast to CPS, the Davidson Office at this time appears to be a functioning company that conducts legitimate business. The seizure of the Davidson Office computers or other storage media may limit the ability of the Davidson Office to conduct its other, apparently legitimate, business. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on the scene what Davidson Office computers or storage media must be seized or copied, and what Davidson Office computers or storage media need not be seized or copied. Law enforcement personnel will speak with Davidson Office personnel on the scene as may be appropriate to this. Where appropriate, law enforcement personnel will copy data, rather than physically seize computers, to reduce the extent of any disruption of the Davidson Office's business operations. If representatives of the Davidson Office so request, the agents will, to the extent practicable, attempt to provide them with copies of data that may be necessary or important to the continued functioning of

the Davidson Office's legitimate business. If, after inspecting the seized computers off-site, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the Government will return it.

Review of Electronically Stored Information

42. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

43. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory

examination of each document in a file cabinet to determine its relevance);

- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files;

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation;[2] and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation.

44. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

45. It may be necessary for programmers and other outside experts to assist the Secret Service during the examination of the computer evidence.

---

[2] Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

Return of Electronically Stored Information

46. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

47. In light of the confidential nature of the continuing investigation, the Government respectfully requests that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

48. Based on the foregoing, I respectfully request the Court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

WHEREFORE, your deponent respectfully requests that search warrant be issued, pursuant to Federal Rule of Criminal Procedure 41, authorizing Secret Service agents, with assistance

from other law enforcement officers, if necessary, to enter the two SUBJECT PREMISES, and therein search for and seize from any location within the SUBJECT PREMISES, the items listed in Attachments B and C, all of which constitute evidence relating to and instrumentalities of the TARGET OFFENSES. Your deponent further requests that the search warrant authorize the opening of any locked or unlocked door, compartment or other object in

[redacted]

ndon McCaw
ret Service

Honorable Steven M. Gold
United States Magistrate Judge
Eastern District of New York

ATTACHMENT A

The Subject Premises:

1. The two SUBJECT PREMISES include the CPS PREMISES and the DAVIDSON PREMISES. Both SUBJECT PREMISES are inside a one-story, light grey building located at 1465 Broadway, Hewlett, New York ("the Building"). As recently as July 21, 2015, the Building had three signs on the exterior bearing the name "Commerce Payment Systems." One sign faces Broadway, while the other two face the reserved-for-tenants parking lot on the left side of the building. The Building has a single, main entrance, which is accessed through the parking lot on the left (northeast) side of the building. There is a secondary entrance on the front of the building, facing Broadway, which opens directly into the office of Michael Mendlowitz, the CEO of CPS. There is also another secondary entrance on the rear right-hand side of the Building.

2. The SUBJECT PREMISES include each computer or other storage medium and any closed or locked container therein.

3. The CPS PREMISES include approximately six distinct areas within the Building: five on the ground floor (the main area, the computer/server room, the front cubicles, and the office of Michael Mendlowitz) as well as most of the basement of the building, and further include

a. The main area. When entering the Building through the main door adjacent to the parking lot, the main area of the CPS PREMISES is straight ahead, mostly behind a reception area and wall. The main area fills a large essentially rectangular space, extending from the main entrance to the opposite wall, and from the right wall (adjacent to Broadway) to the left wall at the rear of the Building.

b. The computer/server room. Along the left-hand (southeast) wall of the main area of the CPS PREMISES is a short hall going to the left. Off that hall, on the right-hand side, is the computer/server room. On the left-hand side of that hall is a set of stairs that leads down to the basement.

c. The basement. A portion of the CPS PREMISES is in the basement of the Building. After one descends the stairs mentioned in the preceding paragraph, one encounters a file storage room on the immediate left, with an adjacent storage area. The next two rooms contain CPS's customer service and shipping departments, each of which also has an adjacent storage area.

d. The front cubicles. Back on the ground floor, if one turns left upon entering the main door of the building from the parking lot, the front cubicles are on the left. Several yards beyond that are three computers and cubicles belonging to employees engaged in the "boarding" process, by which customer profiles are created and loaded with customer-specific information, including fee information.

e. The office of Michael Mendlowitz. Along the right-hand, northwest wall of the main area, adjacent to Broadway, is the office of Michael Mendlowitz. It is approximately the fifth room along that wall, after two one-room offices of other businesses, a CPS conference room, and one more one-room office of another business.

4. The DAVIDSON PREMISES are the one-room office of accountant Michael Davidson, who heads his own accounting business in the Building, within the CPS suite of offices. Immediately to the right after one enters the CPS PREMISES via the main door of the Building from the parking lot, are the one-room DAVIDSON PREMISES, as indicated on Attachment D.

5. In addition to the SUBJECT PREMISES, the ground floor of the Building contains approximately six small one-room business offices leased by other small businesses, as shaded in gray on Attachment D. These are not within the ambit of this application. One of these small offices is on the immediate right as one enters the building through the main entrance from the parking lot. Three more - as described in the preceding sub-paragraph - are along the right-hand, northwest wall of the building, facing Broadway, as is a CPS conference room (the third room). The other two one-room businesses leased by outside entities are toward the left as one enters the building through the main entrance, adjacent to the front cubicles described above.

ATTACHMENT B

PROPERTY TO BE LOCATED AND SEIZED WITHIN THE "CPS PREMISES," KNOWN AND DESCRIBED AS THE PREMISES OF "COMMERCE PAYMENT SYSTEMS," a/k/a "COMMERCE PAYMENT GROUP," a/k/a "MERCHANT COMMERCE," a/k/a "EMPIRE PAYMENTS," a/k/a/ "EVOLUTION BANKCARD," a/k/a "OPTIMAL BANKCARD," AT 1465 BROADWAY, HEWLETT, NEW YORK AND CLOSED CABINETS AND CONTAINERS FOUND INSIDE

The items to be seized from the CPS Premises include the following evidence, fruits, and instrumentalities of the operation of a fraudulent credit-card and debit-card processing scheme in violation of Title 18, United States Code, Sections 1343 and 1349 ("the Target Offenses"):

1. business and financial reports and records, bank and credit card records, customer contracts and applications, customer bills, customer billing profiles, sales and debt-collection records, employee records and files, call logs, call lists, service and other contracts, recorded telephone calls, creditor and debtor records, internal and external correspondence and communications, mail, and payment records, among other documents, stored media and records

2. checks (personal and certified), customer contracts and agreements, customer bills, copies of canceled checks, cash, money orders, records of credit card payments, mail, mail envelopes, correspondences, communications, faxes, emails, phone records (including digital and/or VOIP records), receipts, invoices, general journals, ledgers, financial reports, spreadsheets, memoranda, and notes.

3. Bank account and transaction documents, including account opening documents, ATM and/or debit cards, bank statements, and bank deposit and withdrawal slips;

4. Customer and/or debtor lists, customer and/or debtor files, lists of names, addresses, social security numbers, contact information, bank account numbers, credit card numbers and other personal identifying information, records of communications with customers and/or debtors;

5. Company policies, manuals, instructions, and/or scripts;

6. Any documents mentioning arrests and/or warrants;

7. Licenses and/or registrations;

8. Documents, records and policies regarding employee compensation, such as bonuses and/or commissions;

9. Payroll records, employee names, personnel files;

10. Documents or records bearing the names "Commerce Payment Systems," "Commerce Payment Group," "Merchant Commerce," "Empire Payments," "Evolution Bankcard," "Optimal Bankcard,"

"EVO Merchant Services," "EVO Payments International," "Michael Mendlowitz," or similar names;

11. Records relating to and communications regarding lenders, creditors and/or other sources of information regarding debtors or debts to be collected; and

12. Computer(s), computer hardware, software, related documentation, and passwords.

Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in paragraphs 1 through 12 of this Attachment, above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, scanners, routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

Review of Electronically Stored Information

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the

status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Paragraphs 1-12 of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

ATTACHMENT C

PROPERTY TO BE LOCATED AND SEIZED WITHIN THE "DAVIDSON PREMISES," KNOWN AND DESCRIBED AS THE PREMISES OF THE OFFICE OF MICHAEL DAVIDSON, CERTIFIED PUBLIC ACCOUNTANT, AT 1465 BROADWAY, HEWLETT, NEW YORK AND CLOSED CABINETS AND CONTAINERS FOUND INSIDE

The items to be seized from the Davidson Premises include the following evidence, fruits, and instrumentalities of the operation of a fraudulent credit-card and debit-card processing scheme in violation of Title 18, United States Code, Sections 1343 and 1349 ("the Subject Offenses"):

Any and all documents relating to or bearing the name(s) "Commerce Payment Systems," "Commerce Payment Group," "Merchant Commerce," "Empire Payments," "Evolution Bankcard," "Optimal Bankcard," "EVO Merchant Services," "EVO Payments International," "Michael Mendlowitz," or similar names, including:

1. business and financial reports and records, bank and credit card records, customer contracts and applications, customer bills, customer billing profiles, sales and debt-collection records, employee records and files, call logs, call lists, service and other contracts, recorded telephone calls, creditor and debtor records, internal and external correspondence and communications, mail, and payment records, among other documents, stored media and records

2. checks (personal and certified), customer files, customer contracts and agreements, customer bills, copies of canceled checks, cash, money orders, records of credit card payments, mail, mail envelopes, correspondences, communications, faxes, emails, phone records (including digital and/or VOIP records), receipts, invoices, general journals, ledgers, financial reports, spreadsheets, memoranda, and notes.

3. Bank account and transaction documents, including account opening documents, ATM and/or debit cards, bank statements, and bank deposit and withdrawal slips;

4. Customer and/or debtor lists, customer and/or debtor files, lists of names, addresses, social security numbers, contact information, bank account numbers, credit card numbers and other personal identifying information, records of communications with customers and/or debtors;

5. Company policies, manuals, instructions, and/or scripts;

6. Any documents mentioning arrests and/or warrants;

7. Licenses and/or registrations;

8. Documents, records and policies regarding employee compensation, such as bonuses and/or commissions;

9. Payroll records, employee names, personnel files;

10. Records relating to and communications regarding lenders, creditors and/or other sources of information regarding debtors or debts to be collected; and

11. Computer(s), computer hardware, software, related documentation, and passwords.

Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in paragraphs 1 through 12 of this Attachment, above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, scanners, routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

4. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

5. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

6. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

Review of Electronically Stored Information

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement

personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

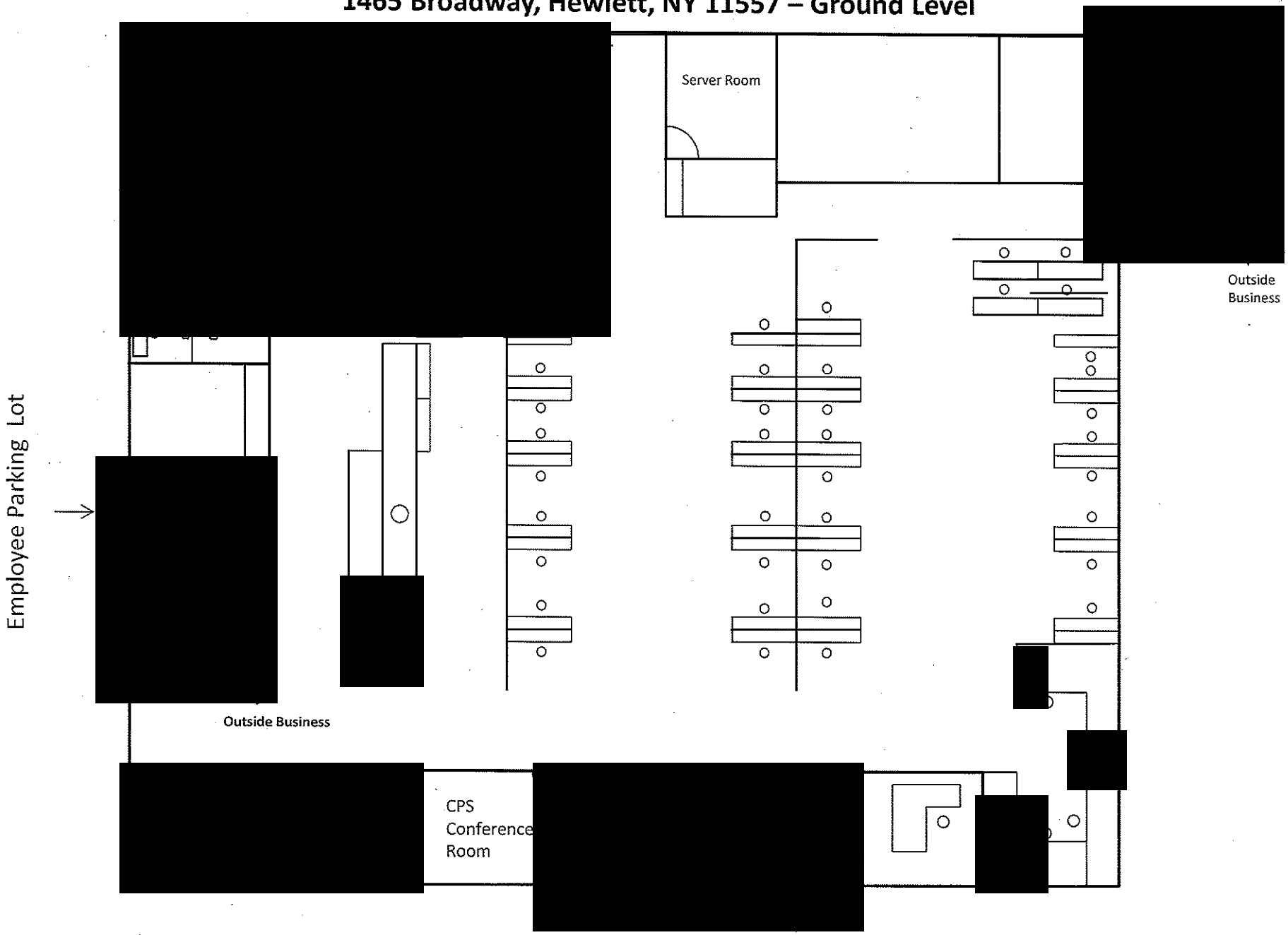
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Paragraphs 1-12 of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

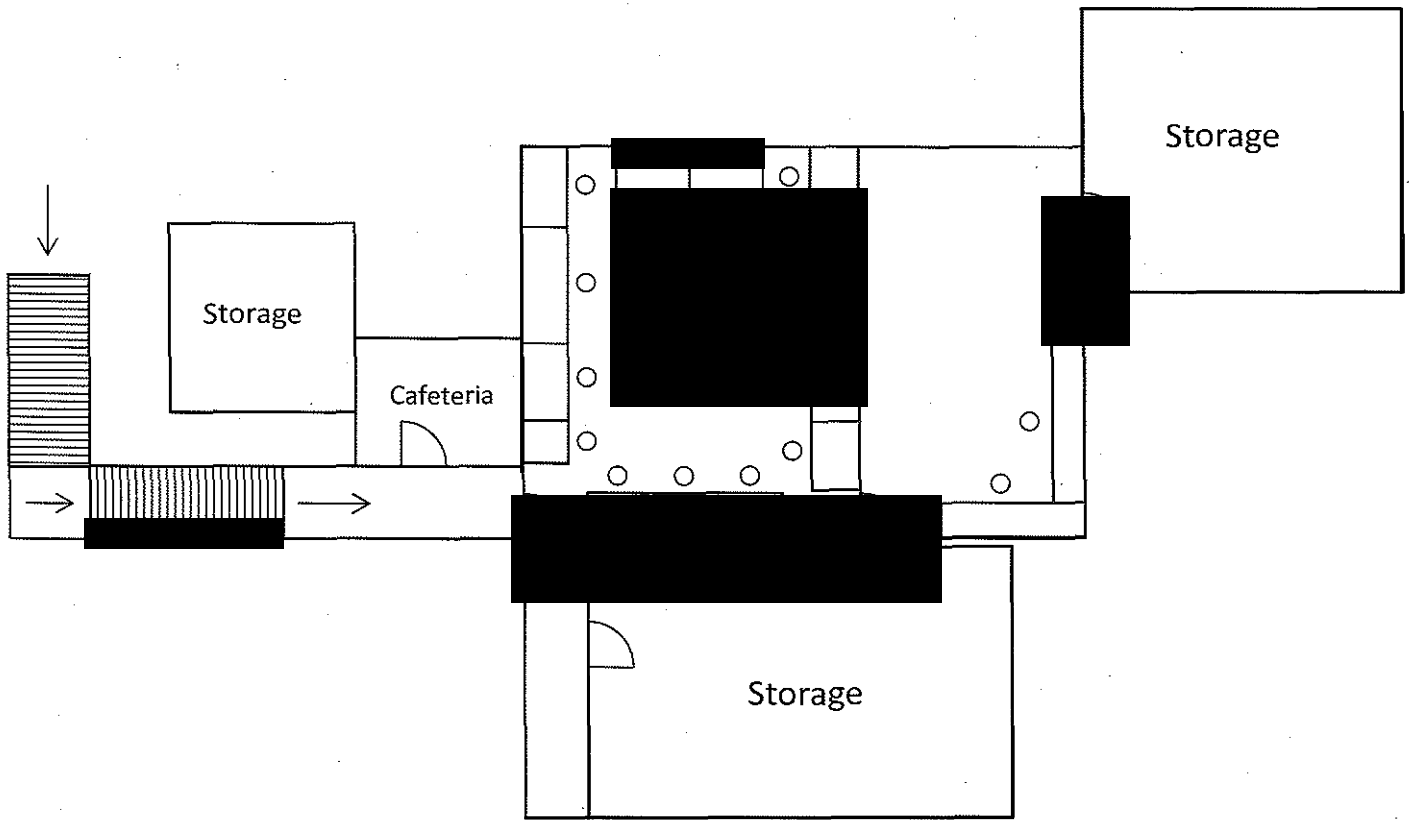
1465 Broadway, Hewlett, NY 11557 – Ground Level



(NOT TO SCALE, NUMBER OF DESKS APPROXIMATE)

ATTACHMENT D

1465 Broadway, Hewlett, NY 11557 – Basement Level



(NOT TO SCALE, NUMBER OF DESKS APPROXIMATE)

COMMERCE
PAYMENT SYSTEMS
COMMERCE

COMMERCE
PAYMENT SYSTEMS
002796

P-393